Clase 2 — 16.10.25

#virtualbox #ciscopackettracer #activedirectory #windowserver

---

🧠 Configuración de Active Directory y Red de Dominio

🗓️ Clase 2 — 16/10/2025
Profesor: Carlos Quintana
Módulo: Ciberseguridad
Tema: Administración y configuración de red en entornos Windows Server

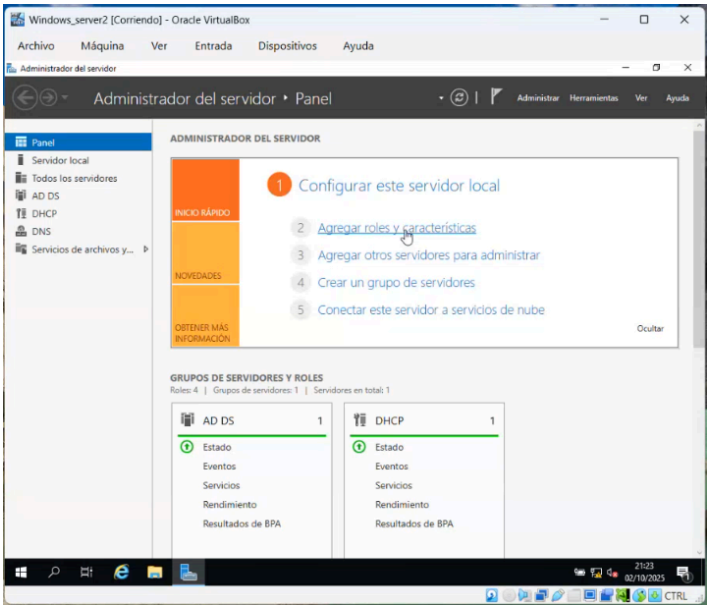
---

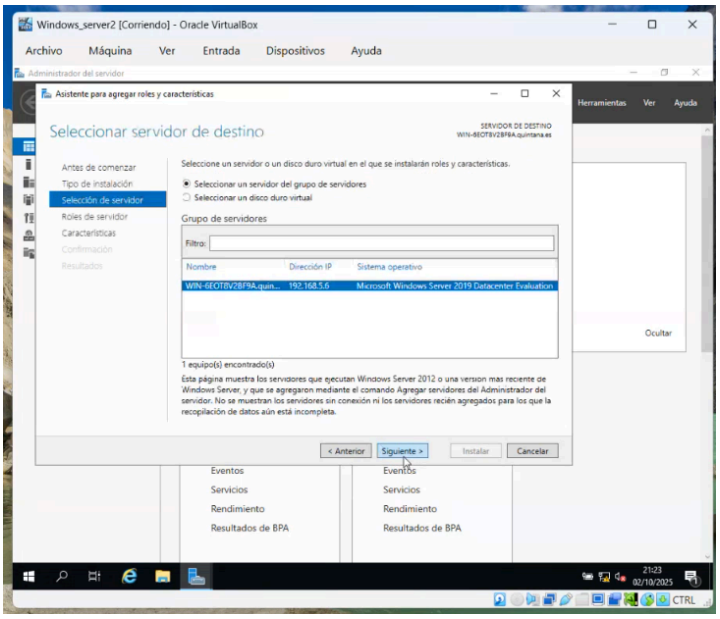
1️⃣ Repaso inicial y configuración de Active Directory

Antes de comenzar con la nueva configuración, el profesor realiza un repaso del proceso visto en la clase anterior:
tras instalar **Windows Server** de forma virtual (mediante Oracle VirtualBox), el primer paso necesario para centralizar la gestión de usuarios y equipos dentro de una red corporativa es **instalar y configurar el rol de Active Directory Domain Services (AD DS)**.

Para iniciar el proceso:

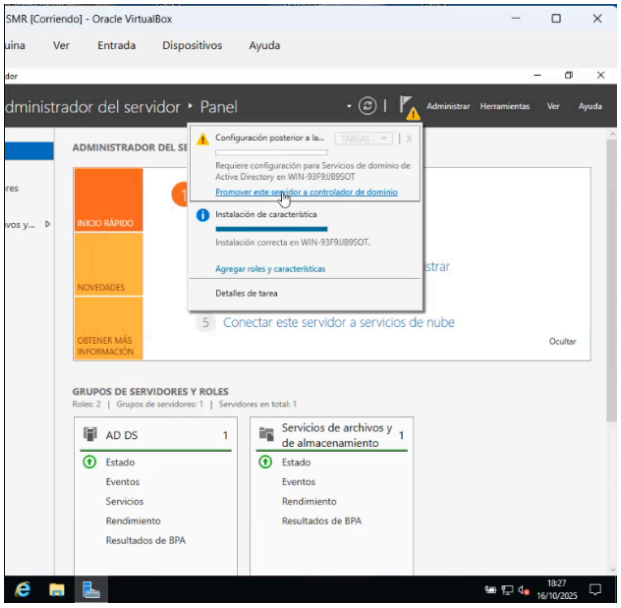
1. Accedemos al **Administrador del servidor**.
2. Seleccionamos **Agregar roles y características**.





3. Avanzamos con *Siguiente* → *Siguiente* hasta llegar al apartado de roles.
4. Activamos **Servicios de dominio de Active Directory (AD DS)**.

Al completar la instalación, se muestra una notificación indicando que es necesario **promover el servidor a controlador de dominio**. Este paso convierte la máquina virtual en el **centro del dominio**, desde el cual se controlarán todas las demás máquinas conectadas a él.



> 💬 **Comentario del profesor:**
> Esta configuración inicial determina que todas las máquinas dependientes del servidor **quedarán vinculadas al dominio central**. Cualquier usuario o equipo que opere bajo este dominio **será gestionado y controlado** desde el Windows Server.

2️⃣ Promoción a controlador de dominio y creación del bosque

En la ventana del asistente de configuración, el profesor selecciona la tercera opción:
“Agregar un nuevo bosque”, lo que implica crear una estructura de dominio completamente nueva (por ejemplo, `alumnos.es` o `quintana.es`).

Los pasos del asistente son los siguientes:

1. **Agregar nuevo bosque:** se define el nombre del dominio raíz.

2. **Contraseña del modo de restauración:** se asigna una clave de recuperación que permitirá restaurar el servicio de directorio en caso de fallo grave.
3. **DNS:** en esta etapa se configura el servicio DNS interno (opcionalmente puede hacerse después).
4. **Nombre NetBIOS:** identificador corto del dominio (por ejemplo, QUINTANA).
5. **Rutas de almacenamiento:** se definen las ubicaciones para las bases de datos y los logs del Active Directory.
6. **Instalación final:** se completa la configuración y se reinicia el servidor.

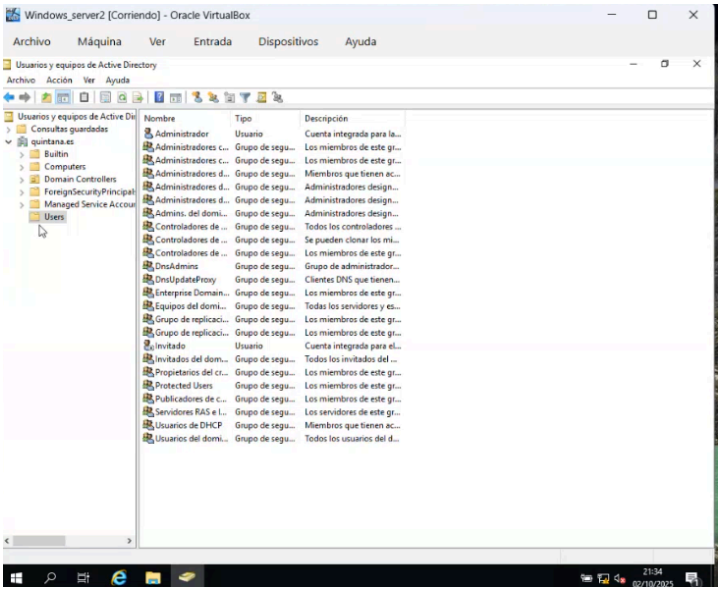
Una vez promovido a **controlador de dominio**, el servidor asume el rol de **autoridad principal** dentro de la red local.

> 💬 **Comentario del profesor:**
> El **controlador de dominio (Domain Controller)** es el corazón del sistema.
> Si esta máquina se apaga, los demás equipos **no podrán autenticarse ni acceder a recursos del dominio**.
> Todo equipo o usuario depende de este servidor mientras la relación de dominio permanezca activa.

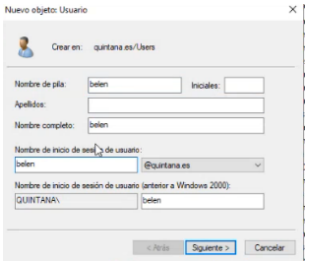
3️⃣ Gestión de usuarios y grupos en Active Directory

Tras la instalación, desde el menú **Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**, se accede a la consola principal de gestión.
Aquí el profesor crea una nueva cuenta de usuario:

1. Carpeta **Users → Clic derecho → Nuevo → Usuario.**



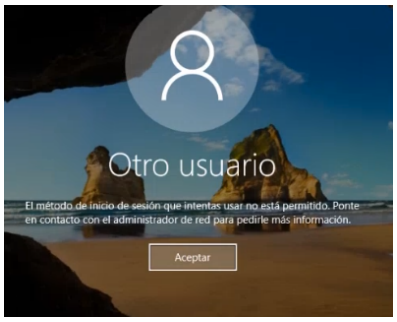
2. Se define el nombre y el inicio de sesión (por ejemplo: `belen@quintana.es`).



3. Se configura una contraseña que cumpla con la política de seguridad del dominio:
   - No puede ser igual al nombre del usuario.
   - Debe incluir **mayúsculas y números** (y preferiblemente símbolos).

4. Se marca la opción **“El usuario debe cambiar la contraseña en el siguiente inicio de sesión”** (recomendado en entornos reales).

El profesor aclara que, si intentamos iniciar sesión con esta nueva cuenta desde otro equipo (por ejemplo, un Windows 10), el acceso fallará inicialmente, ya que el usuario **no tiene permisos de inicio de sesión** en el servidor por defecto.



Para solucionarlo hay dos opciones:

- **Incluir el usuario en un grupo con privilegios elevados** (por ejemplo, “Operadores de cuentas” o “Administradores”).
- **Modificar una GPO (Group Policy Object)** para permitir que el usuario inicie sesión desde ese servidor o equipo concreto.

> 💬 **Comentario del profesor:**
> La política de contraseñas es estricta en entornos de servidor.
> Además, los usuarios sin privilegios deben **pertenecer a un grupo con derechos de inicio de sesión** o no podrán acceder.
> Una mala configuración de grupos o GPO puede dejar fuera incluso a usuarios válidos.

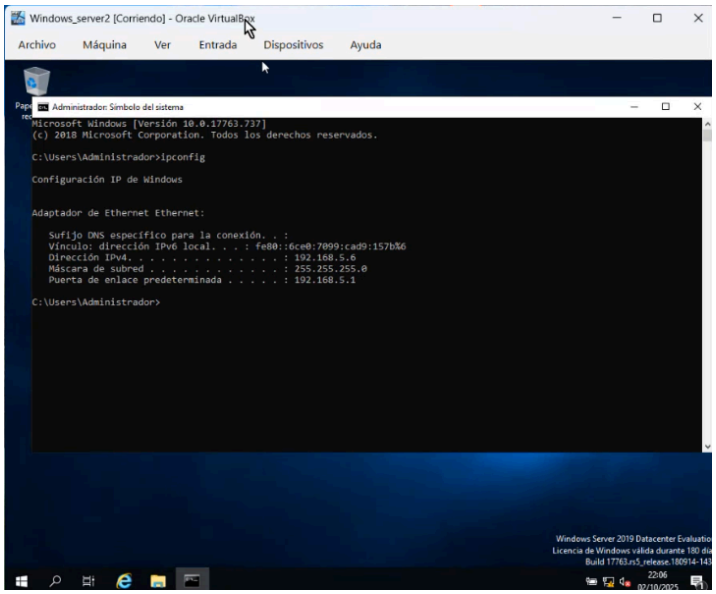
4️⃣ Configuración de red y vinculación con Windows 10

El siguiente paso es conectar una máquina **Windows 10** al dominio administrado por el Windows Server.

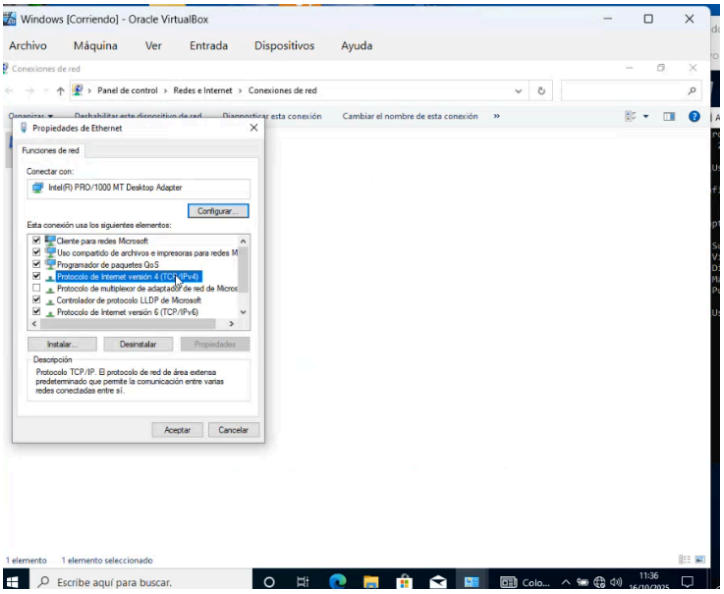
1. En **Windows Server (Administrador)**, se abre el **Símbolo del sistema (cmd)** y se ejecuta:

```
ipconfig
```

```
El resultado muestra:

- IPv4: 192.168.5.6

- Máscara: 255.255.255.0

- Puerta de enlace: 192.168.5.1
```



2. En **Windows 10 (cliente)**, abrimos **Panel de control → Centro de redes → Cambiar configuración del adaptador → Ethernet → Propiedades → IPv4**.



   Se marca “Usar la siguiente dirección IP" y se rellenan los campos:

   - IP: `192.168.5.2`
   - Máscara: `255.255.255.0`
   - Puerta de enlace: **192.168.5.6** (IP del servidor)
   - DNS preferido: **192.168.5.6**

Esto permite que ambos equipos estén **en la misma red** y que el cliente reconozca al servidor como su **DNS y puerta de acceso principal**.

3. Se ejecuta desde el cliente:

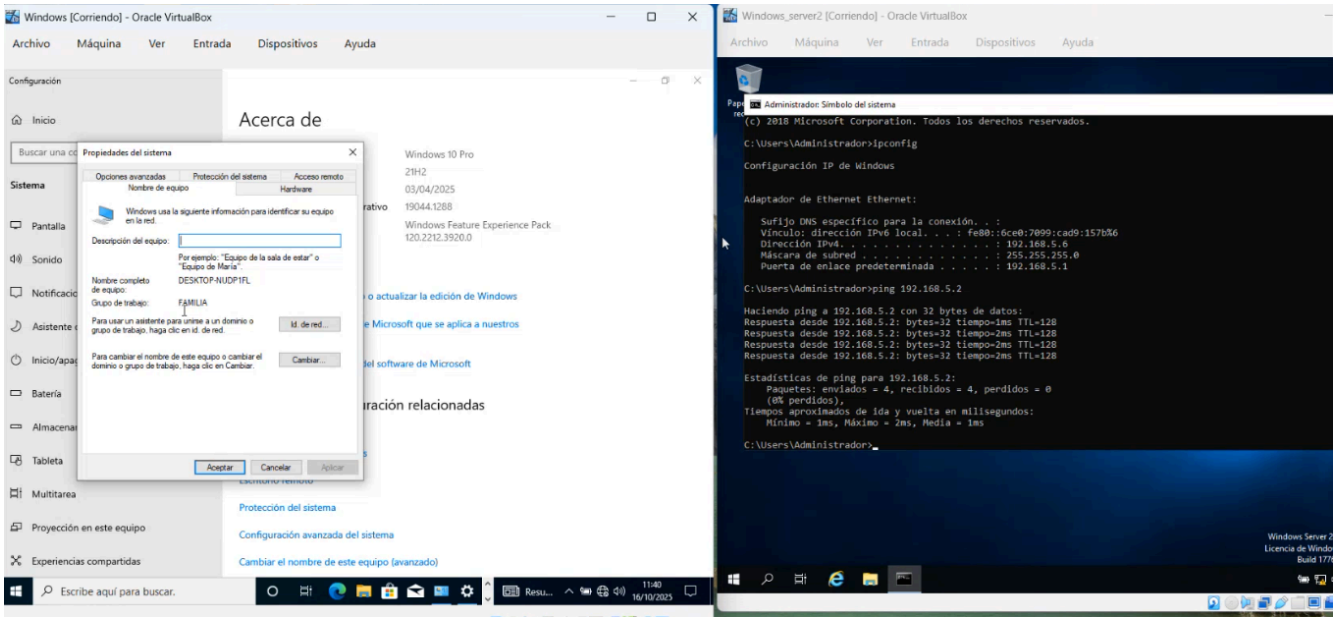
```
ping 192.168.5.6
```

Si responde, la comunicación es correcta.

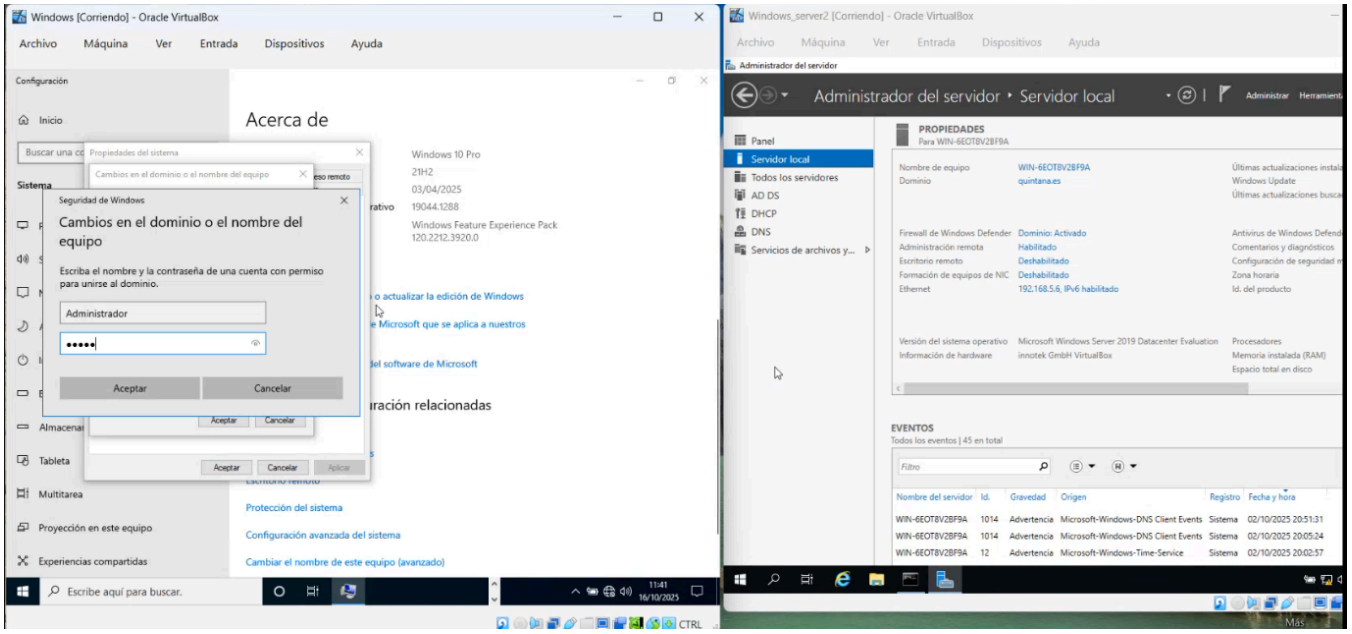
4. En el **Centro de redes → Configuración de uso compartido avanzado**, se debe activar:
   - “Activar la detección de redes”.
   - “Activar el uso compartido de archivos e impresoras”.

Sin estas opciones, la comunicación y descubrimiento entre equipos no funcionará.

5. Finalmente, desde **Propiedades del sistema → Nombre del equipo → Cambiar**, se selecciona **Dominio** e introducimos el nombre del dominio (`quintana.es`).



6. El sistema pedirá credenciales de un usuario con permisos (por ejemplo, `Administrador`). Tras aceptar, será necesario **reiniciar** la máquina.



7. Una vez hecho esto, el Windows 10 **pasa a formar parte del dominio**, quedando subordinado al servidor.

> 💬 **Comentario del profesor:**
> Cuando un equipo entra en un dominio, **“vive para el servidor”**.
> Si el servidor está apagado, el cliente solo podrá usar sus recursos locales, sin conexión a red ni acceso a archivos compartidos.
> En entornos reales, los servidores permanecen **siempre encendidos y vigilados**.

5️⃣ Pruebas de conectividad (IPConfig y Ping)

El profesor realiza una verificación práctica:

1. En Windows Server:

```
ipconfig
```

para confirmar la IP y la puerta de enlace.

2. En Windows 10:

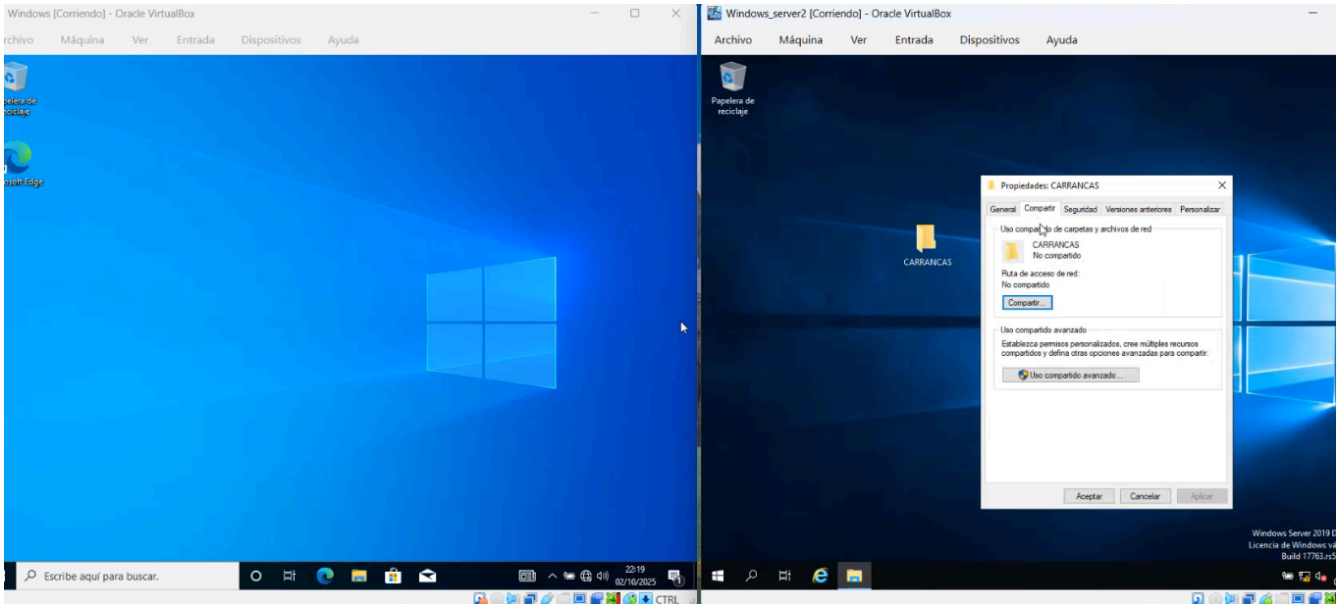
```
ipconfig
ping 192.168.5.6
```

El resultado muestra **0% de pérdida** y tiempos de respuesta estables (1-2 ms), confirmando la comunicación correcta entre cliente y servidor.

> 💬 **Comentario del profesor:**
> Las pruebas con `ipconfig` y `ping` son básicas pero críticas.
> Si no hay respuesta, se revisa primero el **firewall, la configuración IPv4 y el DNS**.
> En entornos virtualizados, pueden surgir errores de red; lo más rápido suele ser **reiniciar la máquina virtual**.

6️⃣ Compartición de recursos en red (carpetas y permisos)

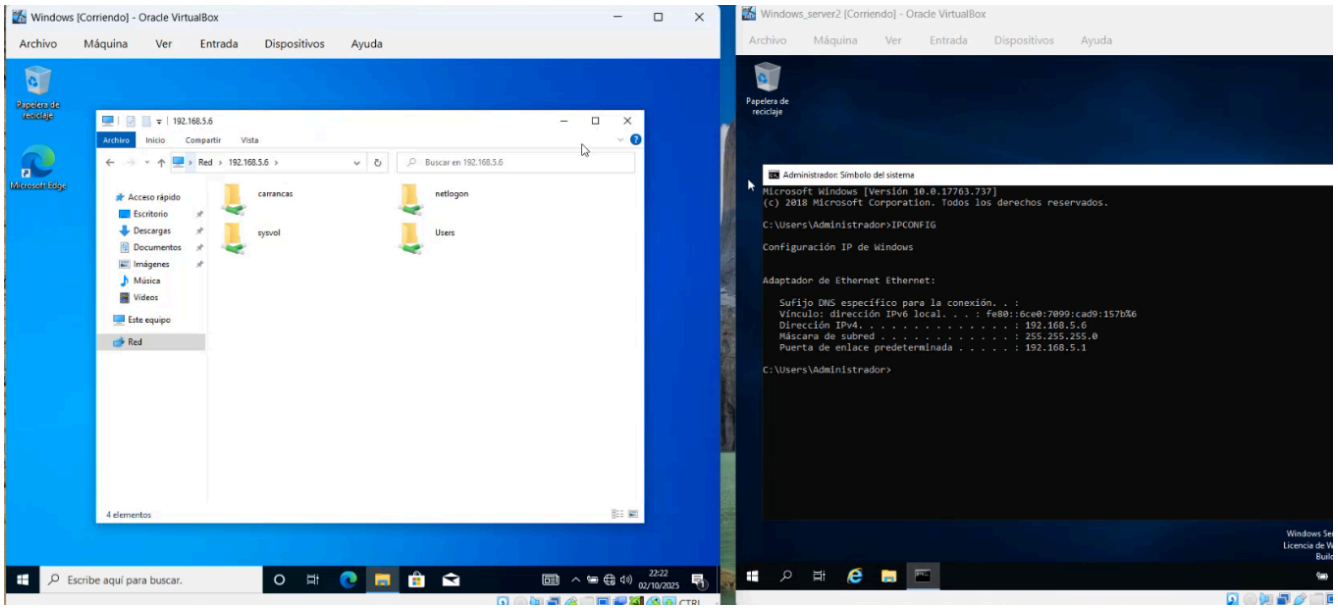
Desde el **Windows Server**, el profesor crea una carpeta (por ejemplo, `CARRANCAS`) y accede a sus propiedades:



1. Pestaña **Compartir → Compartir…**
2. Selecciona los usuarios o grupos que podrán acceder al recurso.
3. Asigna permisos:
   - **Lectura:** el usuario solo puede ver los archivos.
   - **Lectura y escritura:** puede modificar y guardar.
   - **Control total:** puede gestionar todo el contenido.

Una vez compartida, desde el **Windows 10** se puede acceder mediante:

```
\\192.168.5.6\
```



donde aparecerán las carpetas compartidas del servidor (`CARRANCAS` , `Users` , `SYSVOL` , etc.).
También se puede crear un acceso directo para no escribir la ruta manualmente.

> 💬 **Comentario del profesor:**
> Compartir carpetas en red **requiere control de permisos**.
> No todos los usuarios deben tener acceso a todos los recursos.
> El administrador debe establecer políticas seguras, especialmente en entornos corporativos.

7️⃣ Responsabilidad del administrador del dominio

El **administrador del dominio** tiene autoridad total sobre la red y puede crear, eliminar o modificar cualquier cuenta o recurso.
Por ello, existen distintos **niveles jerárquicos** de permisos:

- **Administrador de dominio:** control absoluto de toda la red y servidores.
- **Administrador local:** solo controla su propio equipo.
- **Operador de cuentas:** puede crear, modificar o eliminar usuarios, pero no administradores.

> **REGLA DE ORO:**
> Nunca se usa la **cuenta nativa de “Administrador”** para el trabajo diario.
> Se debe crear una cuenta personalizada (por ejemplo, “jaime_admin”) para tareas habituales y reservar la nativa solo para emergencias.

> 💬 **Comentario del profesor:**
> La seguridad depende del **buen uso de privilegios**.
> Un error del administrador puede afectar a toda la red.
> Siempre deben existir cuentas alternativas para recuperación en caso de fallo o corrupción del dominio.

8️⃣ Anexo técnico — Comandos de red y configuración VirtualBox

🔹 Comandos básicos de red

Comando	Descripción
`ipconfig`	Muestra la configuración IP del equipo.
`ping [IP]`	Comprueba la conectividad entre dos dispositivos.
`hostname`	Muestra el nombre del equipo.
`nslookup [dominio]`	Consulta el DNS configurado.
`net view \\[IP]`	Muestra los recursos compartidos de otro equipo.

🔹 Configuración en VirtualBox

- Ambos sistemas (Server y Cliente) deben estar configurados en **modo Adaptador de red interno** o **red puente**.
- Si las máquinas no se detectan entre sí, reiniciar VirtualBox y comprobar las IP asignadas.
- Para copiar archivos entre las máquinas, puede usarse una carpeta compartida local o red simulada.

> 💬 **Comentario del profesor:**
> En entornos virtuales, la red puede volverse inestable.
> Si algo falla, **reiniciar las máquinas** o **comprobar el modo de red** suele resolver la mayoría de errores de conexión.

✅ Final clase 2

9️⃣ Ampliación teórica

🔹 Concepto general de Active Directory (AD)

Active Directory (AD) es un servicio de directorio desarrollado por Microsoft que permite centralizar la administración de usuarios, equipos y recursos dentro de una red corporativa.
Funciona como una base de datos jerárquica que almacena información sobre todos los objetos de una organización y permite aplicar políticas, autenticar usuarios y controlar permisos desde un punto centralizado.

Componentes principales

Elemento	Descripción
Dominio	Unidad básica de organización en AD. Contiene usuarios, grupos, equipos y políticas. Ejemplo: `quintana.es`.
Árbol	Conjunto de dominios relacionados jerárquicamente que comparten un espacio de nombres común.
Bosque	Conjunto de uno o más árboles de dominio que comparten una configuración de seguridad y confianza mutua. Es la unidad lógica más alta.
Unidad organizativa (OU)	Contenedor lógico dentro de un dominio que permite agrupar objetos (usuarios, equipos) y aplicar políticas específicas (GPO).
Objeto	Cualquier entidad gestionada dentro del directorio: usuarios, equipos, impresoras, grupos, etc.

Integración con otros servicios

Active Directory se apoya en otros componentes esenciales:

- **DNS (Domain Name System):** traduce nombres de dominio en direcciones IP dentro del entorno del bosque.
- **Kerberos:** protocolo de autenticación segura que gestiona la identidad de los usuarios dentro del dominio.
- **LDAP (Lightweight Directory Access Protocol):** protocolo estándar para consultar y modificar los objetos almacenados en el directorio.

> **Comentario:**
> Comprender la estructura jerárquica de Active Directory es fundamental. El dominio representa la organización, el bosque su entorno global y las OU permiten dividir responsabilidades y aplicar políticas específicas.

🔹 Funcionamiento interno del Controlador de Dominio (DC)

Cuando un servidor se promueve a Controlador de Dominio (Domain Controller), se convierte en el núcleo de autenticación y gestión de identidad.
A partir de ese momento, almacena una copia de la base de datos del directorio y controla el acceso de todos los usuarios y equipos del dominio.

Archivos y servicios implicados

- NTDS.dit: base de datos principal del Active Directory.
- SYSVOL: carpeta compartida que contiene políticas de grupo y scripts de inicio.
- NTFRS / DFSR: servicios que replican las políticas y scripts entre controladores de dominio.
- DNS Server: componente crítico para la resolución de nombres en el dominio.

Jerarquía lógica

```
Bosque
 └── Árbol
      └── Dominio raíz
           ├── Dominio hijo
           │     └── OU (Departamentos, Usuarios)
           └── Grupos y objetos
```

> **Comentario:**
> La promoción a controlador de dominio no solo instala AD DS, sino que crea la estructura interna del directorio y habilita los servicios DNS y Kerberos, que son esenciales para la comunicación dentro del dominio.

🔹 Grupos, permisos y políticas en Active Directory

Active Directory permite agrupar usuarios y equipos para aplicar permisos o políticas de forma masiva. Existen varios tipos de grupos según su función y alcance.

Tipos de grupos

Tipo	Función	Ejemplo
Grupos de seguridad	Controlan permisos sobre recursos y archivos.	Operadores de cuentas, Administradores, Usuarios del dominio.

Tipo	Función	Ejemplo
Grupos de distribución	Usados para listas de correo u organización lógica.	Ventas, Soporte técnico.

Ámbito del grupo

Alcance	Descripción
Global	Contiene usuarios del mismo dominio y puede asignarse permisos en otros dominios.
Local de dominio	Puede incluir usuarios o grupos de cualquier dominio, pero sus permisos solo aplican en el dominio donde se crea.
Universal	Puede contener usuarios y grupos de cualquier dominio dentro del bosque.

Políticas de grupo (GPO)

Las GPO (Group Policy Objects) permiten controlar configuraciones de usuarios y equipos dentro del dominio:

- Forzar contraseñas complejas.
- Restringir acceso al Panel de control.
- Impedir instalación de software no autorizado.
- Configurar scripts de inicio de sesión.

Estas políticas pueden aplicarse a nivel de sitio, dominio o unidad organizativa (OU).

Principio del menor privilegio (PoLP)

Cada usuario debe tener solo los permisos estrictamente necesarios para realizar sus tareas.
Este principio reduce el riesgo de errores humanos y ataques internos.

> **Comentario:**
> La administración de permisos debe ser planificada cuidadosamente. Las GPO son potentes, pero una configuración errónea puede bloquear usuarios válidos o dejar brechas de seguridad.

🔹 Permisos de red y sistema de archivos

En un entorno Windows Server, los permisos funcionan en dos niveles:

1. **Permisos de compartición:** controlan el acceso a través de la red.
   - Lectura
   - Cambio (lectura y escritura)
   - Control total
2. **Permisos NTFS:** controlan el acceso directo en el sistema de archivos local.
   - Lectura, escritura, ejecución, modificación, eliminación, etc.

Interacción entre ambos niveles

Cuando un archivo o carpeta tiene configurados ambos tipos de permisos, el más restrictivo prevalece.

Compartición	NTFS	Resultado efectivo
Control total	Lectura	Lectura
Lectura	Control total	Lectura
Cambio	Modificación	Modificación

> **Comentario:**
> En la práctica, se otorgan permisos amplios en la compartición (por ejemplo, Control total) y se afinan los permisos en NTFS, donde hay mayor precisión y seguridad.

🔹 Buenas prácticas del administrador de dominio

- No utilizar la cuenta nativa “Administrador” en el día a día. Crear una cuenta personalizada con permisos equivalentes.
- Realizar copias de seguridad periódicas del dominio y de la base de datos NTDS.dit.
- Aplicar políticas de contraseñas seguras y bloqueo por intentos fallidos.
- Supervisar los registros del Visor de eventos (Event Viewer) para detectar inicios de sesión anómalos.
- Separar roles de administración: un administrador de red no debe tener los mismos privilegios que un administrador de dominio.

> **Comentario:**
> La seguridad de un dominio depende de la disciplina del administrador.
> Un dominio mal gestionado puede comprometer toda la infraestructura de la organización.
